T S7/5/1

7/5/1
DIALOG(R)File 351:Derwent WPI

013608276
WPI Acc No: 2001-092484/200111
XRPX Acc No: N01-069981
Electronic storage device for guaranteeing originality of electronic data varies level of access based on if data are original data or not
Patent Assignee: RICOH KK (RICO)
Inventor: KANAI Y; YACHIDA M
Number of Countries: 002 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 10024753	A1	20001221	DE 1024753	A	20000519	200111	B
JP 2000339223	A	20001208	JP 99145340	A	19990525	200113	
JP 2001005728	A	20010112	JP 99173371	A	19990618	200118	
JP 2001147898	A	20010529	JP 99328802	A	19991118	200136	
JP 2001154577	A	20010608	JP 99338741	A	19991129	200138	
JP 2001209582	A	20010803	JP 200015092	A	20000124	200150	
JP 2001209581	A	20010803	JP 200015091	A	20000124	200150	

Priority Applications (No Type Date): JP 200015092 A 20000124; JP 99145340 A 19990525; JP 99173371 A 19990618; JP 99328802 A 19991118; JP 99338741 A 19991129; JP 200015091 A 20000124
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 10024753	A1		159	G06F-012/14	
JP 2000339223	A		29	G06F-012/14	
JP 2001005728	A		46	G06F-012/14	
JP 2001147898	A		11	G06F-015/00	
JP 2001154577	A		12	G09C-001/00	
JP 2001209582	A		18	G06F-012/14	
JP 2001209581	A		16	G06F-012/14	

Abstract (Basic): DE 10024753 A1

NOVELTY - The storage device includes a storage unit which stores electronic data consisting of a number of content files as a single original in an identifiable state. An access unit controls the access to the original electronic data at a level which is different from the level of access to non-original electronic data. The storage unit stores tamper detection information as original information corresponding to the electronic data.

DETAILED DESCRIPTION - The storage device may include a tamper detection information computing device which receives a request to re-store the electronic data as a single original using an encryption key to compute tamper detection information for each of the content files. A second tamper detection information computing device uses the encryption key to compute second temper detection information for edition management information. INDEPENDENT CLAIMS are included for an electronic storage device, an authorization verification system, an electronic storage method, an authorization verification method, damage recovery method and a storage medium for storing a program in a computer.

USE - For originality-guarantee electronic preservation systems using large-capacity storage media.

ADVANTAGE - Allows the originality of a combined document comprising multiple files to be guaranteed.

```
        pp; 159 DwgNo 0/74
Title Terms: ELECTRONIC; STORAGE; DEVICE; GUARANTEE; ELECTRONIC; DATA; VARY
  ; LEVEL; ACCESS; BASED; DATA; ORIGINAL; DATA
Derwent Class: P85; T01
International Patent Class (Main): G06F-012/14; G06F-015/00
International Patent Class (Additional): G06F-003/06; G06F-009/06;
  G06F-012/00; G06F-012/16; G06F-017/30; G06F-017/60; G09C-001/00
File Segment: EPI; EngPI
?
```

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－209582
（P2001－209582A）
(43)公開日　平成13年８月３日(2001.8.3)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ　５Ｂ０１７

審査請求　未請求　請求項の数21　ＯＬ　（全 18 頁）

(21)出願番号　特願2000－15092(P2000－15092)

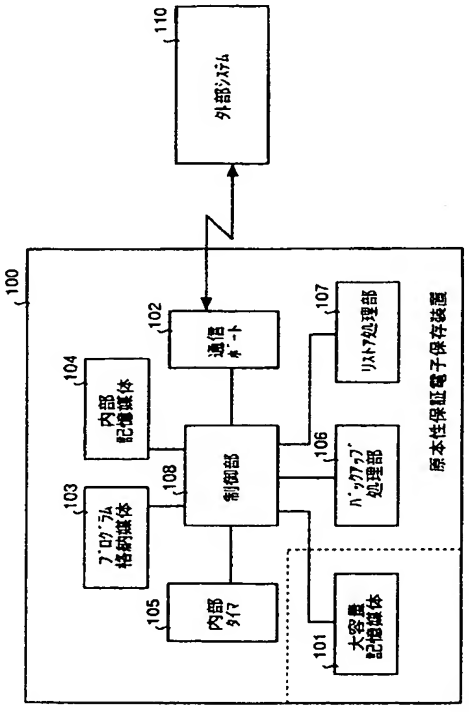
(22)出願日　平成12年１月24日(2000.1.24)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100104190
弁理士　酒井　昭徳

Ｆターム(参考)　5B017 AA05 BA07 CA16

(54)【発明の名称】　原本性保証電子保存装置、障害復旧方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証すること。
【解決手段】　外部システム１１０からバックアップ要求を受け付けた際に、バックアップ処理手段１０６が、内部記憶媒体１０４に格納した管理情報についてのバックアップを作成し、また、外部システム１１０からリストア要求を受け付けた際に、リストア処理部１０７が、バックアップ処理部１０６によって生成されたバックアップ情報を内部記憶媒体１０４にリストアする。



1

【特許請求の範囲】

【請求項１】　内部記憶媒体に格納した所定の管理情報に基づいて大容量記憶媒体に格納した保存データの原本性を保証する原本性保証電子保存装置において、

前記内部記憶媒体に格納した管理情報のバックアップ情報を生成するバックアップ情報生成手段と、

前記内部記憶媒体に格納した管理情報を喪失した場合に、前記バックアップ情報生成手段により生成されたバックアップ情報を前記内部記憶媒体にリストアするリストア手段と、

を備えたことを特徴とする原本性保証電子保存装置。

【請求項２】　前記バックアップ情報生成手段は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することを特徴とする請求項１に記載の原本性保証電子保存装置。

【請求項３】　前記リストア手段は、前記バックアップ情報とともにリストア要求を前記外部システムから受け付けた際に、前記バックアップ情報を前記第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化したバックアップ情報を管理情報として前記内部記憶媒体に記録することを特徴とする請求項２に記載の原本性保証電子保存装置。

【請求項４】　前記バックアップ情報生成手段は、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いて前記バックアップ情報の作成または復号をおこなうことを特徴とする請求項２または３に記載の原本性保証電子保存装置。

【請求項５】　前記バックアップ情報生成手段は、

外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を所定の乱数により暗号化する第１の暗号化手段と、

前記第１の暗号化手段による暗号化に用いた前記乱数を前記第１の暗号鍵により暗号化する第２の暗号化手段と、

前記第１の暗号化手段により暗号化された暗号化管理情報および前記第２の暗号化手段により暗号化された暗号化乱数を前記バックアップ情報として出力する出力手段と、

を備えたことを特徴とする請求項１に記載の原本性保証電子保存装置。

【請求項６】　前記リストア手段は、

前記バックアップ情報に含まれる暗号化乱数を前記第１の復号鍵で復号化する第１の復号化手段と、

前記第１の復号化手段により復号化された乱数で前記暗号化管理情報を復号化する第２の復号化手段と、

前記第２の復号化手段により復号化された管理情報を前記内部記憶媒体に記録する記録手段と、

を備えたことを特徴とする請求項５に記載の原本性保証電子保存装置。

2

【請求項７】　前記出力手段は、

前記第１の暗号化手段により暗号化された暗号化管理情報に前記第２の暗号化手段により暗号化された暗号化乱数を付与して暗号化内部情報を作成する暗号化内部情報作成手段と、前記暗号化内部情報作成手段により作成された暗号化内部情報のハッシュ値を算定する第１のハッシュ値算定手段とを備え、

前記ハッシュ値算定手段により算定されたハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力することを特徴とする請求項５に記載の原本性保証電子保存装置。

【請求項８】　前記リストア手段は、

前記バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定する第２のハッシュ値算定手段と、

前記第２のハッシュ値算定手段により算定されたハッシュ値と前記バックアップ情報に含まれるハッシュ値とを比較する比較手段と、

前記比較手段により両ハッシュ値が一致すると判断された場合に、前記暗号化乱数を前記第１の暗号鍵に対応する第１の復号鍵で復号化する第１の復号化手段と、

前記第１の復号化手段により復号化された乱数を用いて前記暗号化管理情報を復号化する第２の復号化手段と、

を備えたことを特徴とする請求項７に記載の原本性保証電子保存装置。

【請求項９】　前記出力手段は、前記ハッシュ値算定手段により算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力し、

前記比較手段は、前記第２の暗号鍵に対応する第２の復号鍵を用いて前記暗号化ハッシュ値を復号化したハッシュ値と前記第２のハッシュ値算定手段により算定されたハッシュ値とを比較することを特徴とする請求項８に記載の原本性保証電子保存装置。

【請求項１０】　前記第１の暗号鍵および前記第２の復号鍵は公開鍵暗号系の公開鍵であり、前記第２の暗号鍵および前記第１の復号鍵は前記公開鍵暗号系の秘密鍵であることを特徴とする請求項９に記載の原本性保証電子保存装置。

【請求項１１】　内部記憶媒体に格納した所定の管理情報に基づいて大容量記憶媒体に格納した保存データの原本性を保証する原本性保証電子保存装置の障害復旧方法において、

前記内部記憶媒体に格納した管理情報のバックアップ情報を生成するバックアップ情報生成工程と、

前記内部記憶媒体に格納した管理情報を喪失した場合に、前記バックアップ情報生成工程により生成されたバックアップ情報を前記内部記憶媒体にリストアするリス

トア工程と、
を含んだことを特徴とする障害復旧方法。

【請求項１２】　前記バックアップ情報生成工程は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することを特徴とする請求項１１に記載の障害復旧方法。

【請求項１３】　前記リストア工程は、前記バックアップ情報とともにリストア要求を前記外部システムから受け付けた際に、前記バックアップ情報を前記第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化したバックアップ情報を管理情報として前記内部記憶媒体に記録することを特徴とする請求項１２に記載の障害復旧方法。

【請求項１４】　前記バックアップ情報生成工程は、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いて前記バックアップ情報の作成または復号をおこなうことを特徴とする請求項１２または１３に記載の障害復旧方法。

【請求項１５】　前記バックアップ情報生成工程は、
外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を所定の乱数により暗号化する第１の暗号化工程と、
前記第１の暗号化工程による暗号化に用いた前記乱数を前記第１の暗号鍵により暗号化する第２の暗号化工程と、
前記第１の暗号化工程により暗号化された暗号化管理情報および前記第２の暗号化手段により暗号化された暗号化乱数を前記バックアップ情報として出力する出力工程と、
を含んだことを特徴とする請求項１１に記載の障害復旧方法。

【請求項１６】　前記リストア工程は、
前記バックアップ情報に含まれる暗号化乱数を前記第１の復号鍵で復号化する第１の復号化工程と、
前記第１の復号化工程により復号化された乱数で前記暗号化管理情報を復号化する第２の復号化工程と、
前記第２の復号化工程により復号化された管理情報を前記内部記憶媒体に記録する記録工程と、
を含んだことを特徴とする請求項１５に記載の障害復旧方法。

【請求項１７】　前記出力工程は、
前記第１の暗号化工程により暗号化された暗号化管理情報に前記第２の暗号化手段により暗号化された暗号化乱数を付与して暗号化内部情報を作成する暗号化内部情報作成工程と、前記暗号化内部情報作成工程により作成された暗号化内部情報のハッシュ値を算定する第１のハッシュ値算定工程とを含み、
前記ハッシュ値算定工程により算定されたハッシュ値を

前記暗号化内部情報作成工程により作成された暗号化内部情報とともに前記バックアップ情報として出力することを特徴とする請求項１５に記載の障害復旧方法。

【請求項１８】　前記リストア工程は、
前記バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定する第２のハッシュ値算定工程と、
前記第２のハッシュ値算定工程により算定されたハッシュ値と前記バックアップ情報に含まれるハッシュ値とを比較する比較工程と、
前記比較工程により両ハッシュ値が一致すると判断された場合に、前記暗号化乱数を前記第１の暗号鍵に対応する第１の復号鍵で復号化する第１の復号化工程と、
前記第１の復号化工程により復号化された乱数を用いて前記暗号化管理情報を復号化する第２の復号化工程と、
を含んだことを特徴とする請求項１７に記載の障害復旧方法。

【請求項１９】　前記出力工程は、前記ハッシュ値算定工程により算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を前記暗号化内部情報作成工程により作成された暗号化内部情報とともに前記バックアップ情報として出力し、
前記比較工程は、前記第２の暗号鍵に対応する第２の復号鍵を用いて前記暗号化ハッシュ値を復号化したハッシュ値と前記第２のハッシュ値算定工程により算定されたハッシュ値とを比較することを特徴とする請求項１８に記載の障害復旧方法。

【請求項２０】　前記第１の暗号鍵および前記第２の復号鍵は公開鍵暗号系の公開鍵であり、前記第２の暗号鍵および前記第１の復号鍵は前記公開鍵暗号系の秘密鍵であることを特徴とする請求項１９に記載の障害復旧方法。

【請求項２１】　前記請求項１１～２０のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、内部記憶媒体に格納した所定の管理情報に基づいて大容量記憶媒体に格納した保存データの原本性を保証する原本性保証電子保存装置、障害復旧方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特に、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる原本性保証電子保存装置、障害復旧方法および記録媒体に関する。

【０００２】

【従来の技術】近年のコンピュータ技術の進展に伴うペーパーレス化の進展に伴って、紙によって原本書類とし

て保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。

【０００３】たとえば、「金井他：原本性保証電子保存システムの開発－システムの構築－，Medical Imaging Tecnology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発，（特）情報処理振興事業協会発行　創造的ソフトウエア育成事業およびエレクトロニック・コマース推進事業　最終成果発表会論文集　創造的ソフトウエア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。

【０００４】かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、これらの従来技術は、原本となる電子データを格納する大容量記憶媒体以外は、あるレベルの耐タンパー性を持った筐体に格納されていることを前提とするため、原本性保証電子保存装置になんらかの障害が生じた場合に、その障害対処に時間を要する。

【０００６】具体的には、電子データの原本性を保証するためには、内部記憶媒体に記憶した内部管理情報を通常利用することとなるが、この内部記憶媒体に記憶した内部管理情報が障害などによって失われると、耐タンパー性が保持されているためにかえってその復旧に時間を要する結果となる。

【０００７】このため、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる原本性保証電子保存装置をいかに実現するかが極めて重要な課題となっている。

【０００８】この発明は、上記問題（課題）に鑑みてなされたものであり、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる原本性保証電子保存装置、障害復旧方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するために、請求項１に記載の発明にかかる原本性保証電子保存装置は、内部記憶媒体に格納した所定の管理情報に基づいて大容量記憶媒体に格納した保存データの原本性を保証する原本性保証電子保存装置において、前記内部記憶媒体に格納した管理情報のバックアップ情報を生成するバックアップ情報生成手段と、前記内部記憶媒体に格納した管理情報を喪失した場合に、前記バックアップ情報生成手段により生成されたバックアップ情報を前記内部記憶媒体にリストアするリストア手段と、を備えたことを特徴とする。

【００１０】この請求項１に記載の発明によれば、内部記憶媒体に格納した管理情報のバックアップ情報を生成しておき、この内部記憶媒体に格納した管理情報を喪失した場合に、生成されたバックアップ情報を内部記憶媒体にリストアすることとしたので、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる。

【００１１】また、請求項２に記載の発明にかかる原本性保証電子保存装置は、前記バックアップ情報生成手段は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することを特徴とする。

【００１２】この請求項２に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することとしたので、バックアップ情報の暗号強度を高めることができる。

【００１３】また、請求項３に記載の発明にかかる原本性保証電子保存装置は、前記リストア手段は、前記バックアップ情報とともにリストア要求を前記外部システムから受け付けた際に、前記バックアップ情報を前記第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化したバックアップ情報を管理情報として前記内部記憶媒体に記録することを特徴とする。

【００１４】この請求項３に記載の発明によれば、バックアップ情報とともにリストア要求を外部システムから受け付けた際に、バックアップ情報を第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化したバックアップ情報を管理情報として内部記憶媒体に記録することとしたので、暗号化されたバックアップ情報を正しく復号化して内部記憶媒体にリストアすることができる。

【００１５】また、請求項４に記載の発明にかかる原本性保証電子保存装置は、前記バックアップ情報生成手段は、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いて前記バックアップ情報の作成または復号をおこなうことを特徴とする。

【００１６】この請求項４に記載の発明によれば、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いてバックアップ情報の作成または復号をおこなうこととしたので、ＩＣカードに応じて暗号鍵および復号鍵を自在に変更することができる。

【００１７】また、請求項５に記載の発明にかかる原本性保証電子保存装置は、前記バックアップ情報生成手段は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を所定の乱数により暗号化する第１の暗号化手段と、前記第１の暗号化手段による暗号化に用いた前記乱数を前記第１の暗号鍵により暗号化する第２の暗号化手段と、前記第１の暗号化手段により暗号化された暗号化管理情報および前記第２の暗号化手段により暗号化された暗号化乱数を前記バックアップ情報として出力する出力手段と、を備えたことを特徴とする。

【００１８】この請求項５に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を所定の乱数により暗号化し、暗号化に用いた乱数を第１の暗号鍵により暗号化し、暗号化した暗号化管理情報および暗号化乱数をバックアップ情報として出力することとしたので、単に管理情報を暗号化するだけでなく、この暗号化に用いた乱数についても暗号化して出力することができる。

【００１９】また、請求項６に記載の発明にかかる原本性保証電子保存装置は、前記リストア手段は、前記バックアップ情報に含まれる暗号化乱数を前記第１の復号鍵で復号化する第１の復号化手段と、前記第１の復号化手段により復号化された乱数で前記暗号化管理情報を復号化する第２の復号化手段と、前記第２の復号化手段により復号化された管理情報を前記内部記憶媒体に記録する記録手段と、を備えたことを特徴とする。

【００２０】この請求項６に記載の発明によれば、バックアップ情報に含まれる暗号化乱数を第１の復号鍵で復号化し、復号化した乱数で暗号化管理情報を復号化し、この復号化された管理情報を内部記憶媒体に記録することとしたので、暗号化された管理情報を正しく復号化して内部記憶媒体にリストアすることができる。

【００２１】また、請求項７に記載の発明にかかる原本性保証電子保存装置は、前記出力手段は、前記第１の暗号化手段により暗号化された暗号化管理情報に前記第２の暗号化手段により暗号化された暗号化乱数を付与して暗号化内部情報を作成する暗号化内部情報作成手段と、前記暗号化内部情報作成手段により作成された暗号化内部情報のハッシュ値を算定する第１のハッシュ値算定手段とを備え、前記ハッシュ値算定手段により算定されたハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力することを特徴とする。

【００２２】この請求項７に記載の発明によれば、暗号化された暗号化管理情報に暗号化乱数を付与して暗号化内部情報を作成し、作成した暗号化内部情報のハッシュ値を算定し、算定したハッシュ値を暗号化内部情報とともにバックアップ情報として出力することとしたので、暗号化内部情報の改ざんを効率良く防止することができる。

【００２３】また、請求項８に記載の発明にかかる原本性保証電子保存装置は、前記リストア手段は、前記バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定する第２のハッシュ値算定手段と、前記第２のハッシュ値算定手段により算定されたハッシュ値と前記バックアップ情報に含まれるハッシュ値とを比較する比較手段と、前記比較手段により両ハッシュ値が一致すると判断された場合に、前記暗号化乱数を前記第１の暗号鍵に対応する第１の復号鍵で復号化する第１の復号化手段と、前記第１の復号化手段により復号化された乱数を用いて前記暗号化管理情報を復号化する第２の復号化手段と、を備えたことを特徴とする。

【００２４】この請求項８に記載の発明によれば、バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定し、算定したハッシュ値とバックアップ情報に含まれるハッシュ値とを比較し、両ハッシュ値が一致すると判断された場合に、暗号化乱数を第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化した乱数を用いて暗号化管理情報を復号化することとしたので、バックアップ情報が改ざんされているか否かを効率良く判断し、改ざんされていないことを条件として内部記憶媒体への管理情報の設定をおこなうことができる。

【００２５】また、請求項９に記載の発明にかかる原本性保証電子保存装置は、前記出力手段は、前記ハッシュ値算定手段により算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力し、前記比較手段は、前記第２の暗号鍵に対応する第２の復号鍵を用いて前記暗号化ハッシュ値を復号化したハッシュ値と前記第２のハッシュ値算定手段により算定されたハッシュ値とを比較することを特徴とする。

【００２６】この請求項９に記載の発明によれば、算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を暗号化内部情報とともにバックアップ情報として出力し、この第２の暗号鍵に対応する第２の復号鍵を用いて暗号化ハッシュ値を復号化したハッシュ値と算定されたハッシュ値とを比較することとしたので、暗号化ハッシュ値を用いてバックアップ情報の改ざんを防止することができる。

【００２７】また、請求項１０に記載の発明にかかる原本性保証電子保存装置は、前記第１の暗号鍵および前記第２の復号鍵は公開鍵暗号系の公開鍵であり、前記第２の暗号鍵および前記第１の復号鍵は前記公開鍵暗号系の秘密鍵であることを特徴とする。

【００２８】この請求項１０に記載の発明によれば、第１の暗号鍵および第２の復号鍵を公開鍵暗号系の公開鍵とし、第２の暗号鍵および第１の復号鍵を公開鍵暗号系の秘密鍵としたので、公開鍵暗号系を用いてバックアッ

プ情報の暗号強度を高めることができる。

【００２９】また、請求項１１に記載の発明にかかる障害復旧方法は、内部記憶媒体に格納した所定の管理情報に基づいて大容量記憶媒体に格納した保存データの原本性を保証する原本性保証電子保存装置の障害復旧方法において、前記内部記憶媒体に格納した管理情報のバックアップ情報を生成するバックアップ情報生成工程と、前記内部記憶媒体に格納した管理情報を喪失した場合に、前記バックアップ情報生成工程により生成されたバックアップ情報を前記内部記憶媒体にリストアするリストア工程と、を含んだことを特徴とする。

【００３０】この請求項１１に記載の発明によれば、内部記憶媒体に格納した管理情報のバックアップ情報を生成しておき、この内部記憶媒体に格納した管理情報を喪失した場合に、生成されたバックアップ情報を内部記憶媒体にリストアすることとしたので、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる。

【００３１】また、請求項１２に記載の発明にかかる障害復旧方法は、前記バックアップ情報生成工程は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することを特徴とする。

【００３２】この請求項１２に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することとしたので、バックアップ情報の暗号強度を高めることができる。

【００３３】また、請求項１３に記載の発明にかかる障害復旧方法は、前記リストア工程は、前記バックアップ情報とともにリストア要求を前記外部システムから受け付けた際に、前記バックアップ情報を前記第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化したバックアップ情報を管理情報として前記内部記憶媒体に記録することを特徴とする。

【００３４】この請求項１３に記載の発明によれば、バックアップ情報とともにリストア要求を外部システムから受け付けた際に、バックアップ情報を第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化したバックアップ情報を管理情報として内部記憶媒体に記録することとしたので、暗号化されたバックアップ情報を正しく復号化して内部記憶媒体にリストアすることができる。

【００３５】また、請求項１４に記載の発明にかかる障害復旧方法は、前記バックアップ情報生成工程は、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いて前記バックアップ情報の作成または復号をおこなうことを特徴とする。

【００３６】この請求項１４に記載の発明によれば、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いてバックアップ情報の作成または復号をおこなうこととしたので、ＩＣカードに応じて暗号鍵および復号鍵を自在に変更することができる。

【００３７】また、請求項１５に記載の発明にかかる障害復旧方法は、前記バックアップ情報生成工程は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を所定の乱数により暗号化する第１の暗号化工程と、前記第１の暗号化工程による暗号化に用いた前記乱数を前記第１の暗号鍵により暗号化する第２の暗号化工程と、前記第１の暗号化工程により暗号化された暗号化管理情報および前記第２の暗号化手段により暗号化された暗号化乱数を前記バックアップ情報として出力する出力工程と、を含んだことを特徴とする。

【００３８】この請求項１５に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を所定の乱数により暗号化し、暗号化に用いた乱数を第１の暗号鍵により暗号化し、暗号化した暗号化管理情報および暗号化乱数をバックアップ情報として出力することとしたので、単に管理情報を暗号化するだけでなく、この暗号化に用いた乱数についても暗号化して出力することができる。

【００３９】また、請求項１６に記載の発明にかかる障害復旧方法は、前記リストア工程は、前記バックアップ情報に含まれる暗号化乱数を前記第１の復号鍵で復号化する第１の復号化工程と、前記第１の復号化工程により復号化された乱数で前記暗号化管理情報を復号化する第２の復号化工程と、前記第２の復号化工程により復号化された管理情報を前記内部記憶媒体に記録する記録工程と、を含んだことを特徴とする。

【００４０】この請求項１６に記載の発明によれば、バックアップ情報に含まれる暗号化乱数を第１の復号鍵で復号化し、復号化した乱数で暗号化管理情報を復号化し、この復号化された管理情報を内部記憶媒体に記録することとしたので、暗号化された管理情報を正しく復号化して内部記憶媒体にリストアすることができる。

【００４１】また、請求項１７に記載の発明にかかる障害復旧方法は、前記出力工程は、前記第１の暗号化工程により暗号化された暗号化管理情報に前記第２の暗号化手段により暗号化された暗号化乱数を付与して暗号化内部情報を作成する暗号化内部情報作成工程と、前記暗号化内部情報作成工程により作成された暗号化内部情報のハッシュ値を算定する第１のハッシュ値算定工程とを含み、前記ハッシュ値算定工程により算定されたハッシュ値を前記暗号化内部情報作成工程により作成された暗号化内部情報とともに前記バックアップ情報として出力することを特徴とする。

【００４２】この請求項１７に記載の発明によれば、暗号化された暗号化管理情報に暗号化乱数を付与して暗号化内部情報を作成し、作成した暗号化内部情報のハッシュ値を算定し、算定したハッシュ値を暗号化内部情報とともにバックアップ情報として出力することとしたので、暗号化内部情報の改ざんを効率良く防止することができる。

【００４３】また、請求項１８に記載の発明にかかる障害復旧方法は、前記リストア工程は、前記バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定する第２のハッシュ値算定工程と、前記第２のハッシュ値算定工程により算定されたハッシュ値と前記バックアップ情報に含まれるハッシュ値とを比較する比較工程と、前記比較工程により両ハッシュ値が一致すると判断された場合に、前記暗号化乱数を前記第１の暗号鍵に対応する第１の復号鍵で復号化する第１の復号化工程と、前記第１の復号化工程により復号化された乱数を用いて前記暗号化管理情報を復号化する第２の復号化工程と、を含んだことを特徴とする。

【００４４】この請求項１８に記載の発明によれば、バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定し、算定したハッシュ値とバックアップ情報に含まれるハッシュ値とを比較し、両ハッシュ値が一致すると判断された場合に、暗号化乱数を第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化した乱数を用いて暗号化管理情報を復号化することとしたので、バックアップ情報が改ざんされているか否かを効率良く判断し、改ざんされていないことを条件として内部記憶媒体への管理情報の設定をおこなうことができる。

【００４５】また、請求項１９に記載の発明にかかる障害復旧方法は、前記出力工程は、前記ハッシュ値算定工程により算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を前記暗号化内部情報作成工程により作成された暗号化内部情報とともに前記バックアップ情報として出力し、前記比較工程は、前記第２の暗号鍵に対応する第２の復号鍵を用いて前記暗号化ハッシュ値を復号化したハッシュ値と前記第２のハッシュ値算定工程により算定されたハッシュ値とを比較することを特徴とする。

【００４６】この請求項１９に記載の発明によれば、算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を暗号化内部情報とともにバックアップ情報として出力し、この第２の暗号鍵に対応する第２の復号鍵を用いて暗号化ハッシュ値を復号化したハッシュ値と算定されたハッシュ値とを比較することとしたので、暗号化ハッシュ値を用いてバックアップ情報の改ざんを防止することができる。

【００４７】また、請求項２０に記載の発明にかかる障害復旧方法は、前記第１の暗号鍵および前記第２の復号鍵は公開鍵暗号系の公開鍵であり、前記第２の暗号鍵および前記第１の復号鍵は前記公開鍵暗号系の秘密鍵であることを特徴とする。

【００４８】この請求項２０に記載の発明によれば、第１の暗号鍵および第２の復号鍵を公開鍵暗号系の公開鍵とし、第２の暗号鍵および第１の復号鍵を公開鍵暗号系の秘密鍵としたので、公開鍵暗号系を用いてバックアップ情報の暗号強度を高めることができる。

【００４９】また、請求項２１に記載の発明にかかる記録媒体は、前記請求項１１～２０のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項１１～２０の動作をコンピュータによって実現することができる。

【００５０】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかる原本性保証電子保存装置、障害復旧方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【００５１】図１は、本実施の形態において用いる原本性保証電子保存装置の構成を示すブロック図である。同図に示す原本性保証電子保存装置１００は、原本の電子データを大容量記憶媒体１０１上に保持しておき、内部記憶媒体１０４に格納した管理情報などを用いてこの電子データの原本性を保証することようにした装置である。

【００５２】ここで、この原本性保証電子保存装置１００になんらかの障害が発生した場合には、内部記憶媒体１０４に格納した情報が失われてしまい、電子データの原本性を保証することができなくなる。特に、大容量記憶媒体１０１以外は耐タンパー性を持った筐体に格納されるため、管理情報を簡易に再設定することは難しい。

【００５３】このため、この原本性保証電子保存装置１００では、内部記憶媒体１０４に格納した管理情報をバックアップするとともに、この原本性保証電子保存装置１００になんらかの障害が発生した場合には、バックアップした管理情報を内部記憶媒体１０４にリストアするよう構成している。

【００５４】ただし、かかる管理情報は、そもそも原本となる電子データの原本性を保証するために用いるものであり、むやみに装置外部に保持すべきものではないので、その暗号強度を高めることで、本来の原本性保証に影響を与えないようにしている。

【００５５】同図に示すように、この原本性保証電子保存装置１００は、大容量記憶媒体１０１と、通信ポート１０２と、プログラム格納媒体１０３と、内部記憶媒体１０４と、内部タイマ１０５と、バックアップ処理部１０６と、リストア処理部１０７と、制御部１０８とからなる。

【００５６】大容量記憶媒体１０１は、原本となる電子

データなどを記憶する大容量の二次記憶装置であり、たとえば光磁気ディスクやＣＤ－Ｒなどからなる。この大容量記憶媒体１０１は、図中に破線で示したように原本性保証電子保存装置１００から取り外し可能としても良いが、その他の構成部位については原本性保証電子保存装置１００と物理的に一体化し、通信ポート１０２以外からのアクセスを受け付けない耐タンパー性を有する構成にする。

【００５７】ただし、この耐タンパー性には、筐体を開けられないようにシールを貼る程度のレベルから、筐体を開けた場合に装置が動作しなくなるレベルまで様々なものがあるが、本発明はこの耐タンパー性のレベルには特段の制限を受けない。

【００５８】通信ポート１０２は、ネットワークを介して外部システム１１０との通信をおこなうためのインターフェース部であり、たとえばＬＡＮカードなどの通信モデムなどからなる。

【００５９】プログラム格納媒体１０３は、主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを格納したメモリであり、たとえば書換可能なＥＥＰＲＯＭや読み出し専用のＲＯＭなどからなる。

【００６０】内部記憶媒体１０４は、各種プログラムの実行に必要となるパラメータを記憶するＥＥＰＲＯＭなどからなるメモリであり、具体的には、装置暗号鍵、装置復号鍵、媒体認証コードリスト、最新データ識別番号、タイマ設定履歴ファイルおよびアカウント管理リストなどを記憶する。内部タイマ１０５は、制御部１０８の本体をなすプロセッサがプログラムの実行時に所得する時刻を計時するタイマである。

【００６１】バックアップ処理部１０６は、乱数および公開鍵などを用いて内部記憶媒体１０４に格納した管理情報のバックアップ情報を生成する処理部であり、具体的には、内部記憶媒体１０４から装置設定ファイルなどの後述する各種ファイルを読み出して内部管理情報一括データとする。その後、装置内部で乱数を生成してこの乱数を公開鍵で暗号化して、暗号化乱数を作成するとともに、該乱数で内部管理情報一括データを一括して暗号化し、これに暗号化乱数を付与して内部管理情報一括暗号化データとする。

【００６２】その後、この内部管理情報一括暗号化データについてのハッシュ値を計算し、このハッシュ値を秘密鍵で暗号化してプログラム署名を作成し、このプログラム署名を内部管理情報一括暗号化データに付与して、内部管理情報一括パッケージデータを作成して、外部システム１１０に送出する。

【００６３】リストア処理部１０７は、内部記憶媒体１０４に格納した管理情報を喪失した場合に、バックアップ処理部１０６により生成されたバックアップ情報に含まれる管理情報を内部記憶媒体１０４にリストアする処理部である。

【００６４】具体的には、外部システム１１０から内部管理情報一括パッケージデータを受け取ったならば、この内部管理情報一括パッケージデータを内部管理情報一括暗号化データとプログラム署名とに分離し、内部管理情報一括暗号化データのハッシュ値を計算するとともに、プログラム署名を公開鍵で復号化する。

【００６５】そして、両ハッシュ値が一致する場合には、内部管理情報一括暗号化データに含まれる暗号化乱数を秘密鍵で復号化して乱数を取得し、この乱数で内部管理情報一括暗号化データを復号化して内部管理情報一括データを取得し、この内部管理情報一括データを形成する各ファイルを内部記憶媒体１０４に格納する。

【００６６】制御部１０８は、その実体はプロセッサであり、プログラム格納媒体１０３に格納された主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラム、復号化プログラムおよびバックアップ制御プログラムなどの各種プログラムを読み出して実行することになる。

【００６７】具体的には、この制御部１０８では、外部システム１１０などから内部管理情報のバックアップ作成要求を受け付けた際に、バックアップの作成をバックアップ１０６に対して指示するとともに、外部システム１１０などからリストア要求を受け付けた際に、リストア処理部１０７に対してリストア指示をおこなう。

【００６８】なお、本実施の形態では、説明の便宜上外部システム１１０などからの要求に応答してバックアップ並びにリストアをおこなうよう制御することとしたが、内部タイマ１０５の計時に基づいて定期的にバックアップ指示をおこなうとともに、内部記憶媒体１０４の異常を検知してリストア指示をおこなうよう構成することもできる。

【００６９】上記構成を有する原本性保証電子保存装置１００を用いることにより、内部記憶媒体１０４に格納した管理情報を効率良くバックアップするとともに、状況に応じてバックアップ情報を内部記憶媒体１０４に迅速にリストアし、もって大容量記憶媒体１０１に格納した原本の電子データの原本性を継続的に保証することができる。

【００７０】つぎに、図１に示した大容量記憶媒体１０１に保持したファイル並びに内部記憶媒体１０４に保持したファイルについて説明する。図２は、図１に示した大容量記憶媒体１０１上に保持した電子データ並びに内部記憶媒体１０４に保持した管理情報を説明するための説明図である。

【００７１】同図に示すように、大容量記憶媒体１０１には、原本としての各電子データが保存データとして格納されるとともに、その保存データを管理するための保存データリストファイルと、媒体ごとに管理するための媒体管理情報ファイルが格納されている。

15

【００７２】具体的には、この保存データリストファイルは、保存データごとに設けられた複数の保存データエントリからなり、各保存データエントリは、保存データ識別番号、保存データ名、作成情報、最終更新情報、廃棄情報および最新のバージョン番号などで形成される。また、媒体管理情報ファイルは、媒体識別番号、媒体名および媒体初期化日時情報などで形成される。

【００７３】これに対して、内部記憶媒体１０４には、電子署名の計算などに使用する装置固有の装置暗号鍵（公開鍵暗号系の場合には秘密鍵）、電子署名の検証などに用いる装置固有の装置復号鍵（公開鍵暗号系の場合には公開鍵）、保存データ識別番号や媒体識別番号を生成する際に用いる装置識別番号、つぎの保存データに付与する保存データ識別番号、つぎにフォーマットする媒体に付与するつぎの媒体識別番号、大容量記憶媒体１０１の真正性を検証するための媒体認証コードリスト、内部タイマ設定履歴、外部システム１１０のアカウントを管理するアカウント管理リスト並びに装置アクセスログなどを格納する。

【００７４】具体的には、図中に示した装置設定ファイルには、上記装置暗号鍵、装置復号鍵、装置識別情報、つぎの保存データ識別番号およびつぎの媒体識別番号などが記録され、また、媒体認証コードリストファイルには、媒体識別番号および媒体認証コードなどが記録される。さらに、内部タイマ設定履歴ファイルには内部タイマ設定履歴が記録され、装置アクセス履歴ファイルには装置アクセス履歴が記録され、アカウント管理リストファイルにはアカウント管理リストが記録されている。

【００７５】つぎに、図１に示した外部システム１１０からの原本性保証電子保存装置１００へのログイン手順について説明する。図３は、図１に示した外部システム１１０からの原本性保証電子保存装置１００へのログイン手順を示すフローチャートである。

【００７６】まず、内部管理情報のバックアップをおこなう際には、管理者などが外部システム１１０を用いて原本性保証電子保存装置１００に対してログインをしなければならない。なお、ここではパスワードによる一般的なチャレンジレスポンス認証処理をおこなうこととする。

【００７７】同図に示すように、外部システム１１０が、原本性電子保存装置１００に対してアカウント名とログイン要求を送信すると（ステップＳ３０１）、原本性保証電子保存装置１００は、このアカウント名とログイン要求を受信し（ステップＳ３０２）、内部記憶媒体１０４からアカウント管理テーブルを取得し（ステップＳ３０３）、このアカウント管理テーブルから該当するアカウントエントリを取得する（ステップＳ３０４）。

【００７８】そして、該当するエントリが存在するか否かを確認し（ステップＳ３０５）、該当するエントリが存在しない場合（ステップＳ３０５否定）は、エラーの

16

終了コードを外部システム１１０のクライアントに送信し（ステップＳ３０６）、エラー処理をおこなって（ステップＳ３１８）、処理を終了する。

【００７９】これに対して、該当するエントリが存在する場合（ステップＳ３０５肯定）は、乱数を生成し（ステップＳ３０７）、この乱数を外部システム１１０のクライアントに送信するとともに（ステップＳ３０８）、該乱数とアカウントエントリに格納されているユーザ側内部認証鍵を合わせたものに対してハッシュ値を計算する（ステップＳ３０９）。

【００８０】また、外部システム１１０がこの乱数を受信したならば（ステップＳ３１０）、この乱数とパスワードを合わせたものに対してハッシュ値を計算し（ステップＳ３１１）、計算したハッシュ値を原本性保証電子保存装置１００に対して送信する（ステップＳ３１２）。

【００８１】そして、原本性保証電子保存装置１００が、このハッシュ値を受信すると（ステップＳ３１３）、受信したハッシュ値が計算したハッシュ値と一致するか否かを確認し（ステップＳ３１４）、両者が一致しない場合（ステップＳ３１４否定）は、エラーの結果コードをクライアントに送信し（ステップＳ３１５）、エラー処理をおこなって（ステップＳ３１８）、処理を終了する。

【００８２】一方、両者が一致する場合（ステップＳ３１４肯定）には、成功した結果コードを外部システム１１０のクライアントに送信し（ステップＳ３１６）、ログインしたアカウントのアカウントエントリを内部に保持する（ステップＳ３１７）。

【００８３】なお、外部システム１１０が結果コードを受信したならば（ステップＳ３１９）、この結果コードがエラーコードであるか否かを確認し（ステップＳ３２０）、エラーコードである場合（ステップＳ３２０肯定）は、エラー処理をおこなう（ステップＳ３２１）。

【００８４】上記一連の処理をおこなうことにより、外部システム１１０からクライアントがバックアップ要求をおこなうに際して、原本性保証電子保存装置１００に対して正常にログインすることができる。

【００８５】つぎに、図１に示したバックアップ処理部１０６などによるバックアップ手順について説明する。図４は、図１に示したバックアップ処理部１０６などによるバックアップ手順を示すフローチャートである。

【００８６】同図に示すように、原本性保証電子保存装置１００がバックアップ要求を受け付けたならば、内部に保持しているアカウントエントリのアカウント権限を参照し（ステップＳ４０１）、装置管理者のアカウント権限があるか否かを確認する（ステップＳ４０２）。そして、アカウント権限がない場合（ステップＳ４０２否定）は、エラー処理をおこなった後に（ステップＳ４１２）、処理を終了する。

17

【００８７】これに対して、アカウント権限がある場合（ステップＳ４０２肯定）は、内部記憶媒体１０４から装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リストファイルを読み出し（ステップＳ４０３）、読み出したファイルを一括して内部管理情報一括データとする（ステップＳ４０４）。

【００８８】なお、内部記憶媒体１０４に記憶する装置アクセス履歴ファイルについては、外部システム１１０から原本性保証電子保存装置１００へのアクセスが生ずるたびに頻繁に変更されるファイルであるため、ここではこの装置アクセス履歴ファイルのバックアップはおこなわないものとする。

【００８９】その後、装置内部で乱数を生成し（ステップＳ４０５）、この乱数をプログラム内部のプログラム公開鍵で暗号化して暗号化乱数を作成し（ステップＳ４０６）、該乱数により内部管理情報一括データを暗号化し、これに暗号化乱数を付与して内部管理情報一括暗号化データとする（ステップＳ４０７）。

【００９０】その後、この内部管理情報一括暗号化データについてのハッシュ値を計算し（ステップＳ４０８）、このハッシュ値を秘密鍵で暗号化してプログラム署名を作成し（ステップＳ４０９）、このプログラム署名を内部管理情報一括暗号化データに付与して、内部管理情報一括パッケージデータを作成して（ステップＳ４１０）、外部システム１１０に送出する（ステップＳ４１１）。

【００９１】つぎに、図１に示したリストア処理部１０７などによるリストア手順について説明する。図５は、図１に示したリストア処理部１０７などによるリストア手順を示すフローチャートである。なお、ここでは全く新しい原本性保証電子保存装置１００に内部管理情報をリストアする場合を示すこととする。

【００９２】同図に示すように、原本性保証電子保存装置１００がリストア要求を受け付けたならば、内部に保持しているアカウントエントリのアカウント権限を参照し（ステップＳ５０１）、装置管理者のアカウント権限があるか否かを確認する（ステップＳ５０２）。そして、アカウント権限がない場合（ステップＳ５０２否定）は、エラー処理をおこなった後に（ステップＳ５１７）、すべての処理を終了する。

【００９３】これに対して、アカウント権限がある場合（ステップＳ５０２肯定）は、完全に新しい原本性保証電子保存装置１００であるか否かについても確認し（ステップＳ５０３）、新しい原本性保証電子保存装置１００でない場合（ステップＳ５０３否定）は、エラー処理をおこなった後に（ステップＳ５１７）、すべての処理を終了する。

【００９４】一方、新しい原本性保証電子保存装置１００である場合（ステップＳ５０３肯定）は、外部システム１１０から内部管理情報一括パッケージデータを受け取り（ステップＳ５０４）、この内部管理情報一括パッケージデータを内部管理情報一括暗号化データとプログラム署名とに分離し（ステップＳ５０５）、内部管理情報一括暗号化データのハッシュ値を計算するとともに（ステップＳ５０６）、プログラム署名をプログラム内部に保持しているプログラム公開鍵で復号化する（ステップＳ５０７）。

18

【００９５】そして、復号化したものが先のハッシュ値と一致するか否かを確認し（ステップＳ５０８）、両ハッシュ値が一致しない場合（ステップＳ５０８否定）には、エラー処理をおこない（ステップＳ５１７）、その後、すべての処理を終了する。

【００９６】これに対して、両ハッシュ値が一致する場合（ステップＳ５０８肯定）は、内部管理情報一括暗号化データから暗号化乱数を取得し（ステップＳ５０９）、この暗号化乱数をプログラム内部に保持しているプログラム秘密鍵で復号化して乱数を取得し（ステップＳ５１０）、この乱数で内部管理情報一括暗号化データを復号化して内部管理情報一括データを取得し（ステップＳ５１１）、この内部管理情報一括データを分解して、装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リストファイルとして内部記憶媒体１０４に記録する（ステップＳ５１２）。

【００９７】そして、外部システム１１０から受け取った現在時刻で内部タイマ１０５を設定し（ステップＳ５１３）、設定前の日時情報を不明とし、設定後の日時情報を先に受け取った現在時刻に設定したタイマ設定エントリを作成する（ステップＳ５１４）。そして、内部設定履歴ファイルに新しいタイマ設定エントリを追加し（ステップＳ５１５）、装置アクセス履歴ファイルに、リストアしたことを示すログを記録して（ステップＳ５１６）、処理を終了する。

【００９８】ところで、上記処理では、全く新しい原本性保証電子保存装置１００に内部管理情報をリストアすることとしたが、すでに使用している原本性保証電子保存装置１００に相乗りする形で内部管理情報をリストアする場合もある。

【００９９】そこで、つぎに、使用している原本性保証電子保存装置１００に相乗りする形で内部管理情報をリストアする場合のリストア手順について説明する。図６は、図１に示したリストア処理部１０７などが、使用している原本性保証電子保存装置１００に相乗りする形で内部管理情報をリストアする場合のリストア手順を示すフローチャートである。

【０１００】同図に示すように、この場合にも、原本性保証電子保存装置１００がリストア要求を受け付けたならば、内部に保持しているアカウントエントリのアカウント権限を参照し（ステップＳ６０１）、装置管理者の

アカウント権限があるか否かを確認する（ステップＳ６０２）。そして、アカウント権限がない場合（ステップＳ６０２否定）は、エラー処理をおこなった後に（ステップＳ６１６）、処理を終了する。

【０１０１】これに対して、アカウント権限がある場合（ステップＳ６０２肯定）は、外部システム１１０から内部管理情報一括パッケージデータを受け取り（ステップＳ６０３）、この内部管理情報一括パッケージデータを内部管理情報一括暗号化データとプログラム署名とに分離し（ステップＳ６０４）、内部管理情報一括暗号化データのハッシュ値を計算するとともに（ステップＳ６０５）、プログラム署名をプログラム内部に保持しているプログラム公開鍵で復号化する（ステップＳ６０６）。

【０１０２】そして、復号化したものが先のハッシュ値と一致するか否かを確認し（ステップＳ６０７）、両ハッシュ値が一致しない場合（ステップＳ６０７否定）には、エラー処理をおこなった後に（ステップＳ６１６）、処理を終了する。

【０１０３】これに対して、両ハッシュ値が一致する場合（ステップＳ６０７肯定）は、内部管理情報一括暗号化データから暗号化乱数を取得し（ステップＳ６０８）、この暗号化乱数をプログラム内部に保持しているプログラム秘密鍵で復号化して乱数を取得し（ステップＳ６０９）、この乱数で内部管理情報一括暗号化データを復号化して内部管理情報一括データを取得し（ステップＳ６１０）、この内部管理情報一括データを分解して（ステップＳ６１１）、分解して得られた装置設定ファイルから装置識別番号を取得する（ステップＳ６１２）。

【０１０４】そして、装置識別番号を名前とするフォルダを内部記憶媒体１０４に作成し（ステップＳ６１３）、そのフォルダの下に、分解して得られた装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リストファイルとして内部記憶媒体１０４に記録するとともに（ステップＳ６１４）、装置アクセス履歴ファイルに、リストアしたことを示すログを記録して（ステップＳ６１５）、処理を終了する。

【０１０５】上述してきたように、本実施の形態にかかる原本性保証電子保存装置１００では、外部システム１１０からバックアップ要求を受け付けた際に、バックアップ処理手段１０６が、内部記憶媒体１０４に格納した管理情報についてのバックアップを作成し、また、外部システム１１０からリストア要求を受け付けた際に、リストア処理部１０７が、バックアップ処理部１０６によって生成されたバックアップ情報を内部記憶媒体１０４にリストアするよう構成したので、内部記憶媒体１０４に格納した管理情報を効率良くバックアップするとともに、状況に応じてバックアップ情報を内部記憶媒体１０４に迅速にリストアし、もって大容量記憶媒体１０１に格納した原本の電子データの原本性を継続的に保証することができる。

【０１０６】なお、本実施の形態で説明した障害復旧方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーション等のコンピュータまたはマイコン内蔵のプリンタ、ディジタル複写機等で実行することにより実現される。このプログラムは、ＲＡＭ、ＲＯＭ、ハードディスク、フロッピーディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。またこのプログラムは、上記記録媒体を介して、あるいは伝送媒体としてネットワークを介して配布することができる。

【０１０７】

【発明の効果】以上説明したように、請求項１に記載の発明によれば、内部記憶媒体に格納した管理情報のバックアップ情報を生成しておき、この内部記憶媒体に格納した管理情報を喪失した場合に、生成されたバックアップ情報を内部記憶媒体にリストアすることとしたので、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる原本性保証電子保存装置が得られるという効果を奏する。

【０１０８】また、請求項２に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することとしたので、バックアップ情報の暗号強度を高めることができる原本性保証電子保存装置が得られるという効果を奏する。

【０１０９】また、請求項３に記載の発明によれば、バックアップ情報とともにリストア要求を外部システムから受け付けた際に、バックアップ情報を第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化したバックアップ情報を管理情報として内部記憶媒体に記録するよう構成したので、暗号化されたバックアップ情報を正しく復号化して内部記憶媒体にリストアすることができる原本性保証電子保存装置が得られるという効果を奏する。

【０１１０】また、請求項４に記載の発明によれば、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いてバックアップ情報の作成または復号をおこなうよう構成したので、ＩＣカードに応じて暗号鍵および復号鍵を自在に変更することができる原本性保証電子保存装置が得られるという効果を奏する。

【０１１１】また、請求項５に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、

内部記憶媒体に格納した管理情報を所定の乱数により暗号化し、暗号化に用いた乱数を第１の暗号鍵により暗号化し、暗号化した暗号化管理情報および暗号化乱数をバックアップ情報として出力するよう構成したので、単に管理情報を暗号化するだけでなく、この暗号化に用いた乱数についても暗号化して出力することができる原本性保証電子保存装置が得られるという効果を奏する。

【０１１２】また、請求項６に記載の発明によれば、バックアップ情報に含まれる暗号化乱数を第１の復号鍵で復号化し、復号化した乱数で暗号化管理情報を復号化し、この復号化された管理情報を内部記憶媒体に記録するよう構成したので、暗号化された管理情報を正しく復号化して内部記憶媒体にリストアすることができる原本性保証電子保存装置が得られるという効果を奏する。

【０１１３】また、請求項７に記載の発明によれば、暗号化された暗号化管理情報に暗号化乱数を付与して暗号化内部情報を作成し、作成した暗号化内部情報のハッシュ値を算定し、算定したハッシュ値を暗号化内部情報とともにバックアップ情報として出力するよう構成したので、暗号化内部情報の改ざんを効率良く防止することができる原本性保証電子保存装置が得られるという効果を奏する。

【０１１４】また、請求項８に記載の発明によれば、バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定し、算定したハッシュ値とバックアップ情報に含まれるハッシュ値とを比較し、両ハッシュ値が一致すると判断された場合に、暗号化乱数を第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化した乱数を用いて暗号化管理情報を復号化するよう構成したので、バックアップ情報が改ざんされているか否かを効率良く判断し、改ざんされていないことを条件として内部記憶媒体への管理情報の設定をおこなうことができる原本性保証電子保存装置が得られるという効果を奏する。

【０１１５】また、請求項９に記載の発明によれば、算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を暗号化内部情報とともにバックアップ情報として出力し、この第２の暗号鍵に対応する第２の復号鍵を用いて暗号化ハッシュ値を復号化したハッシュ値と算定されたハッシュ値とを比較するよう構成したので、暗号化ハッシュ値を用いてバックアップ情報の改ざんを防止することができる原本性保証電子保存装置が得られるという効果を奏する。

【０１１６】また、請求項１０に記載の発明によれば、第１の暗号鍵および第２の復号鍵を公開鍵暗号系の公開鍵とし、第２の暗号鍵および第１の復号鍵を公開鍵暗号系の秘密鍵とするよう構成したので、公開鍵暗号系を用いてバックアップ情報の暗号強度を高めることができる原本性保証電子保存装置が得られるという効果を奏する。

【０１１７】また、請求項１１に記載の発明によれば、

内部記憶媒体に格納した管理情報のバックアップ情報を生成しておき、この内部記憶媒体に格納した管理情報を喪失した場合に、生成されたバックアップ情報を内部記憶媒体にリストアするよう構成したので、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる障害復旧方法が得られるという効果を奏する。

【０１１８】また、請求項１２に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を第１の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力するよう構成したので、バックアップ情報の暗号強度を高めることができる障害復旧方法が得られるという効果を奏する。

【０１１９】また、請求項１３に記載の発明によれば、バックアップ情報とともにリストア要求を外部システムから受け付けた際に、バックアップ情報を第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化したバックアップ情報を管理情報として内部記憶媒体に記録するよう構成したので、暗号化されたバックアップ情報を正しく復号化して内部記憶媒体にリストアすることができる障害復旧方法が得られるという効果を奏する。

【０１２０】また、請求項１４に記載の発明によれば、装置本体に装着したＩＣカードの内部に保持した第１の暗号鍵および第１の復号鍵を用いてバックアップ情報の作成または復号をおこなうよう構成したので、ＩＣカードに応じて暗号鍵および復号鍵を自在に変更することができる障害復旧方法が得られるという効果を奏する。

【０１２１】また、請求項１５に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を所定の乱数により暗号化し、暗号化に用いた乱数を第１の暗号鍵により暗号化し、暗号化した暗号化管理情報および暗号化乱数をバックアップ情報として出力するよう構成したので、単に管理情報を暗号化するだけでなく、この暗号化に用いた乱数についても暗号化して出力することができる障害復旧方法が得られるという効果を奏する。

【０１２２】また、請求項１６に記載の発明によれば、バックアップ情報に含まれる暗号化乱数を第１の復号鍵で復号化し、復号化した乱数で暗号化管理情報を復号化し、この復号化された管理情報を内部記憶媒体に記録するよう構成したので、暗号化された管理情報を正しく復号化して内部記憶媒体にリストアすることができる障害復旧方法が得られるという効果を奏する。

【０１２３】また、請求項１７に記載の発明によれば、暗号化された暗号化管理情報に暗号化乱数を付与して暗号化内部情報を作成し、作成した暗号化内部情報のハッシュ値を算定し、算定したハッシュ値を暗号化内部情報とともにバックアップ情報として出力するよう構成した

ので、暗号化内部情報の改ざんを効率良く防止することができる障害復旧方法が得られるという効果を奏する。

【０１２４】また、請求項１８に記載の発明によれば、バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定し、算定したハッシュ値とバックアップ情報に含まれるハッシュ値とを比較し、両ハッシュ値が一致すると判断された場合に、暗号化乱数を第１の暗号鍵に対応する第１の復号鍵で復号化し、復号化した乱数を用いて暗号化管理情報を復号化するよう構成したので、バックアップ情報が改ざんされているか否かを効率良く判断し、改ざんされていないことを条件として内部記憶媒体への管理情報の設定をおこなうことができる障害復旧方法が得られるという効果を奏する。

【０１２５】また、請求項１９に記載の発明によれば、算定されたハッシュ値を第２の暗号鍵を用いて暗号化した暗号化ハッシュ値を暗号化内部情報とともにバックアップ情報として出力し、この第２の暗号鍵に対応する第２の復号鍵を用いて暗号化ハッシュ値を復号化したハッシュ値と算定されたハッシュ値とを比較するよう構成したので、暗号化ハッシュ値を用いてバックアップ情報の改ざんを防止することができる障害復旧方法が得られるという効果を奏する。

【０１２６】また、請求項２０に記載の発明によれば、第１の暗号鍵および第２の復号鍵を公開鍵暗号系の公開鍵とし、第２の暗号鍵および第１の復号鍵を公開鍵暗号系の秘密鍵とするよう構成したので、公開鍵暗号系を用いてバックアップ情報の暗号強度を高めることができる障害復旧方法が得られるという効果を奏する。

【０１２７】また、請求項２１に記載の発明にかかる記録媒体は、請求項１１～２０のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項１１～２０の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図１】この実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。

【図２】図１に示した大容量記憶媒体に保持したファイル並びに内部記憶媒体に保持したファイルを説明するための説明図である。

【図３】図１に示した外部システムからの原本性保証電子保存装置へのログイン手順を示すフローチャートである。

【図４】図１に示したバックアップ処理部によるバックアップ手順を示すフローチャートである。

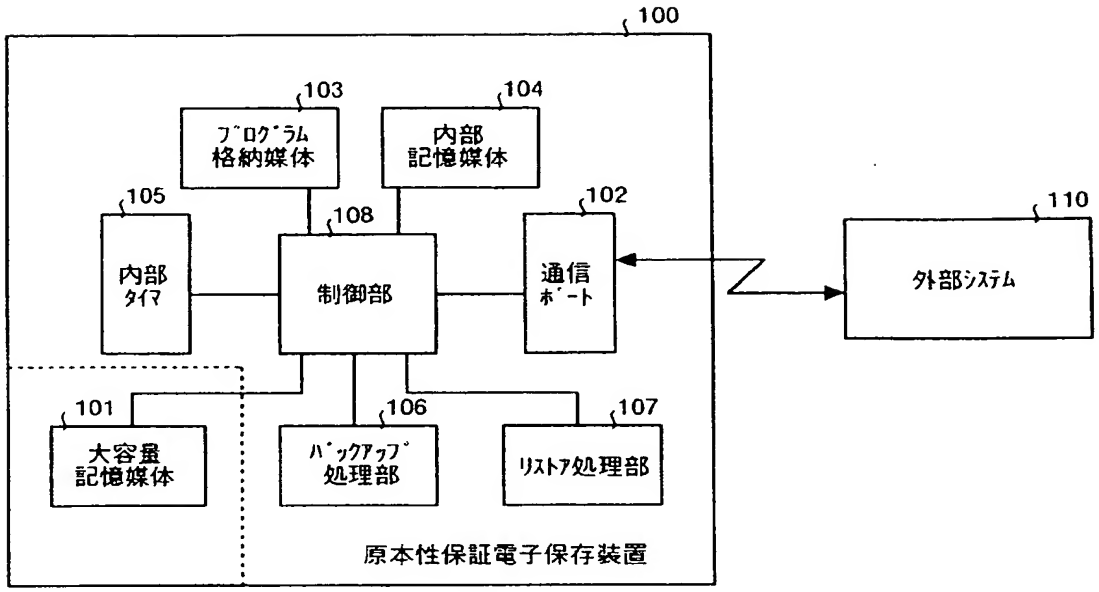
【図５】図１に示したリストア処理部によるリストア手順を示すフローチャートである。

【図６】図１に示したリストア処理部が、使用している原本性保証電子保存装置に相乗りする形で内部管理情報をリストアする場合のリストア手順を示すフローチャートである。

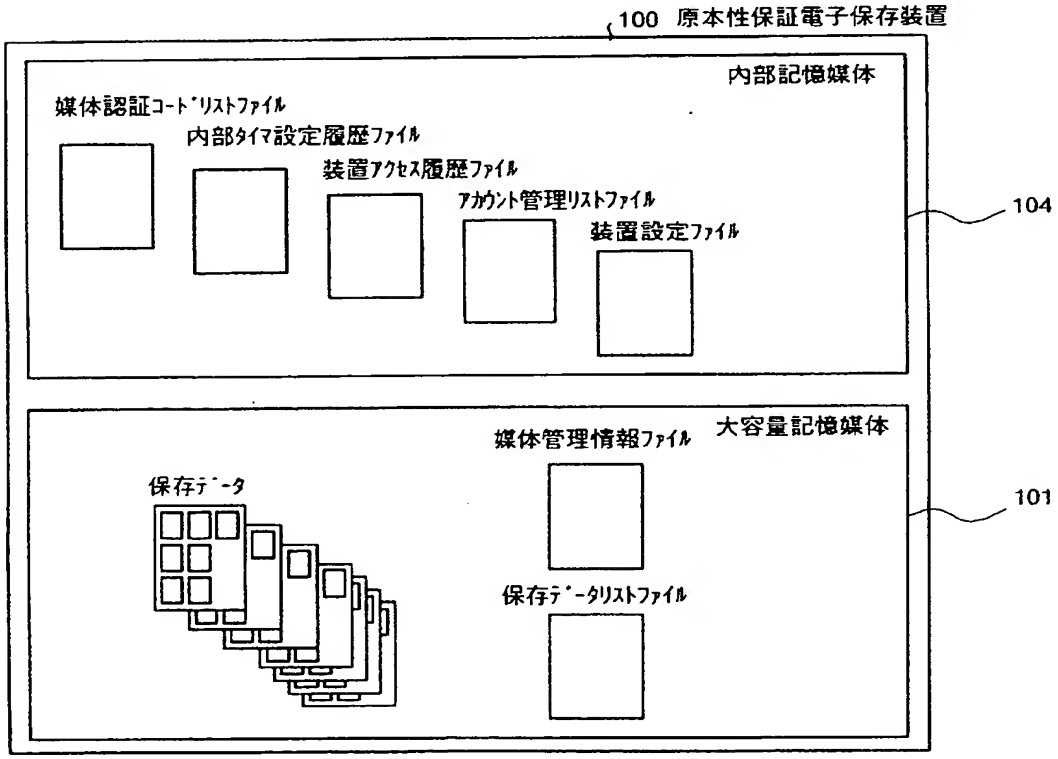
【符号の説明】

１００　原本性保証電子保存装置
１０１　大容量記憶媒体
１０２　通信ポート
１０３　プログラム格納媒体
１０４　内部記録媒体
１０５　内部タイマ
１０６　バックアップ処理部
１０７　リストア処理部
１０８　制御部
１１０　外部システム

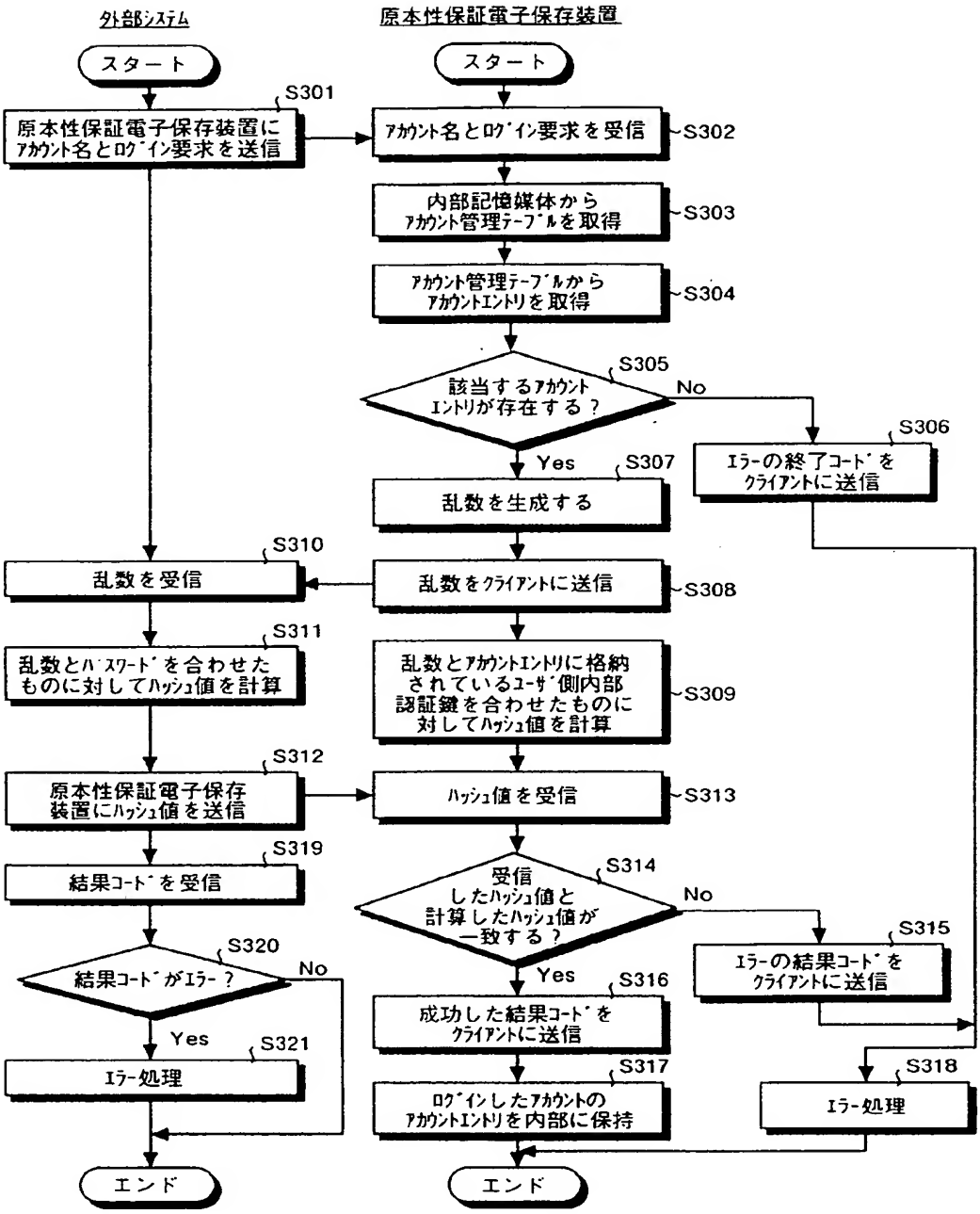
【図１】


100
103
ﾌﾟﾛｸﾞﾗﾑ
格納媒体
104
内部
記憶媒体
105
内部
ﾀｲﾏ
108
制御部
102
通信
ﾎﾟｰﾄ
110
外部ｼｽﾃﾑ
101
大容量
記憶媒体
106
ﾊﾞｯｸｱｯﾌﾟ
処理部
107
ﾘｽﾄｱ処理部
原本性保証電子保存装置

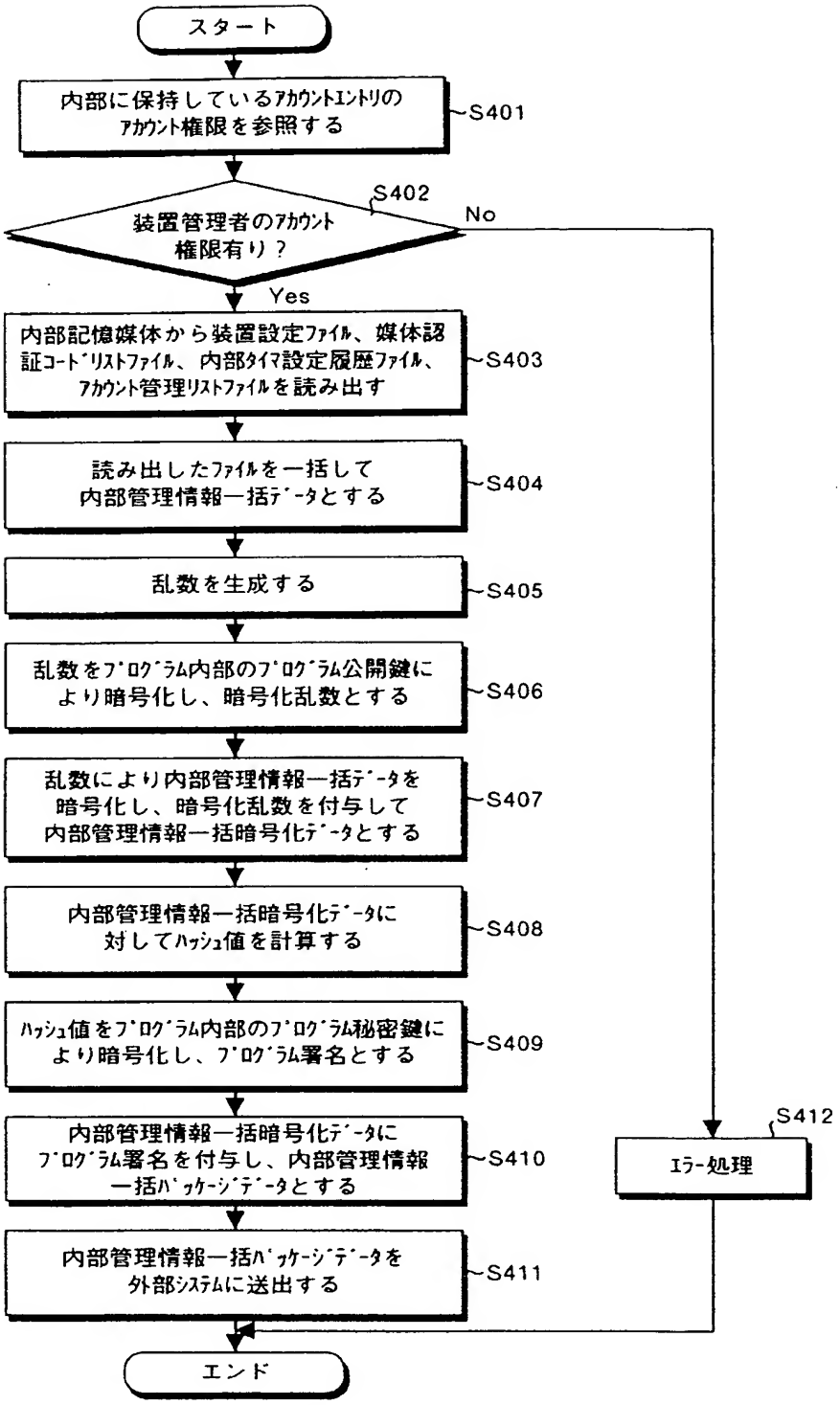
【図２】


100 原本性保証電子保存装置
内部記憶媒体
媒体認証ｺｰﾄﾞﾘｽﾄﾌｧｲﾙ
内部ﾀｲﾏ設定履歴ﾌｧｲﾙ
装置ｱｸｾｽ履歴ﾌｧｲﾙ
ｱｶｳﾝﾄ管理ﾘｽﾄﾌｧｲﾙ
装置設定ﾌｧｲﾙ
104
大容量記憶媒体
媒体管理情報ﾌｧｲﾙ
保存ﾃﾞｰﾀ
保存ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙ
101

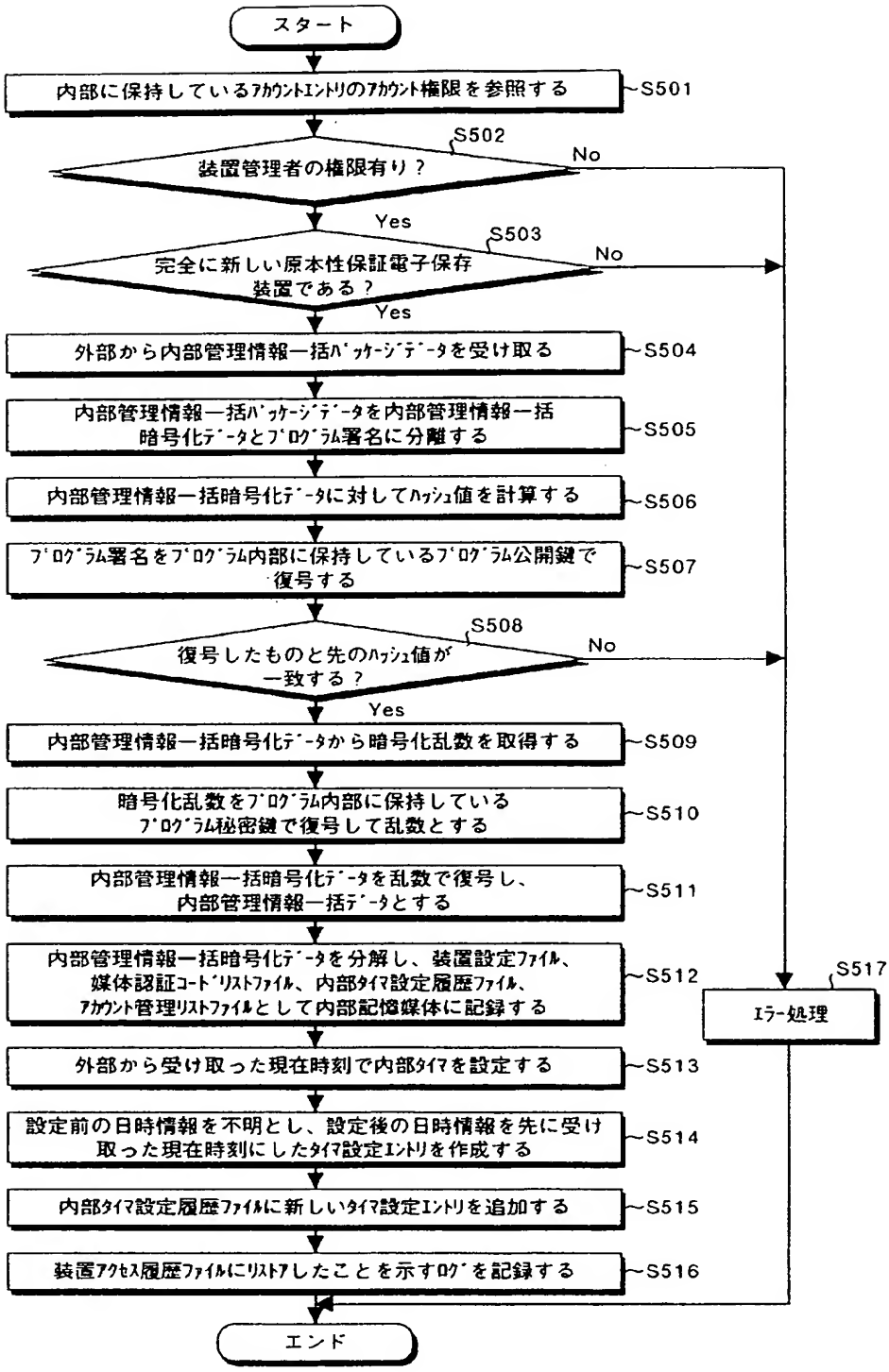
【図３】


外部システム
原本性保証電子保存装置
スタート
スタート
S301
原本性保証電子保存装置にアカウント名とログイン要求を送信
アカウント名とログイン要求を受信
S302
内部記憶媒体からアカウント管理テーブルを取得
S303
アカウント管理テーブルからアカウントエントリを取得
S304
S305
該当するアカウントエントリが存在する？
No
S306
エラーの終了コードをクライアントに送信
Yes
S307
乱数を生成する
S310
乱数を受信
乱数をクライアントに送信
S308
S311
乱数とパスワードを合わせたものに対してハッシュ値を計算
乱数とアカウントエントリに格納されているユーザ側内部認証鍵を合わせたものに対してハッシュ値を計算
S309
S312
原本性保証電子保存装置にハッシュ値を送信
ハッシュ値を受信
S313
S319
結果コードを受信
S314
受信したハッシュ値と計算したハッシュ値が一致する？
No
S315
エラーの結果コードをクライアントに送信
S320
結果コードがエラー？
No
Yes
S316
成功した結果コードをクライアントに送信
Yes
S321
エラー処理
S317
ログインしたアカウントのアカウントエントリを内部に保持
S318
エラー処理
エンド
エンド

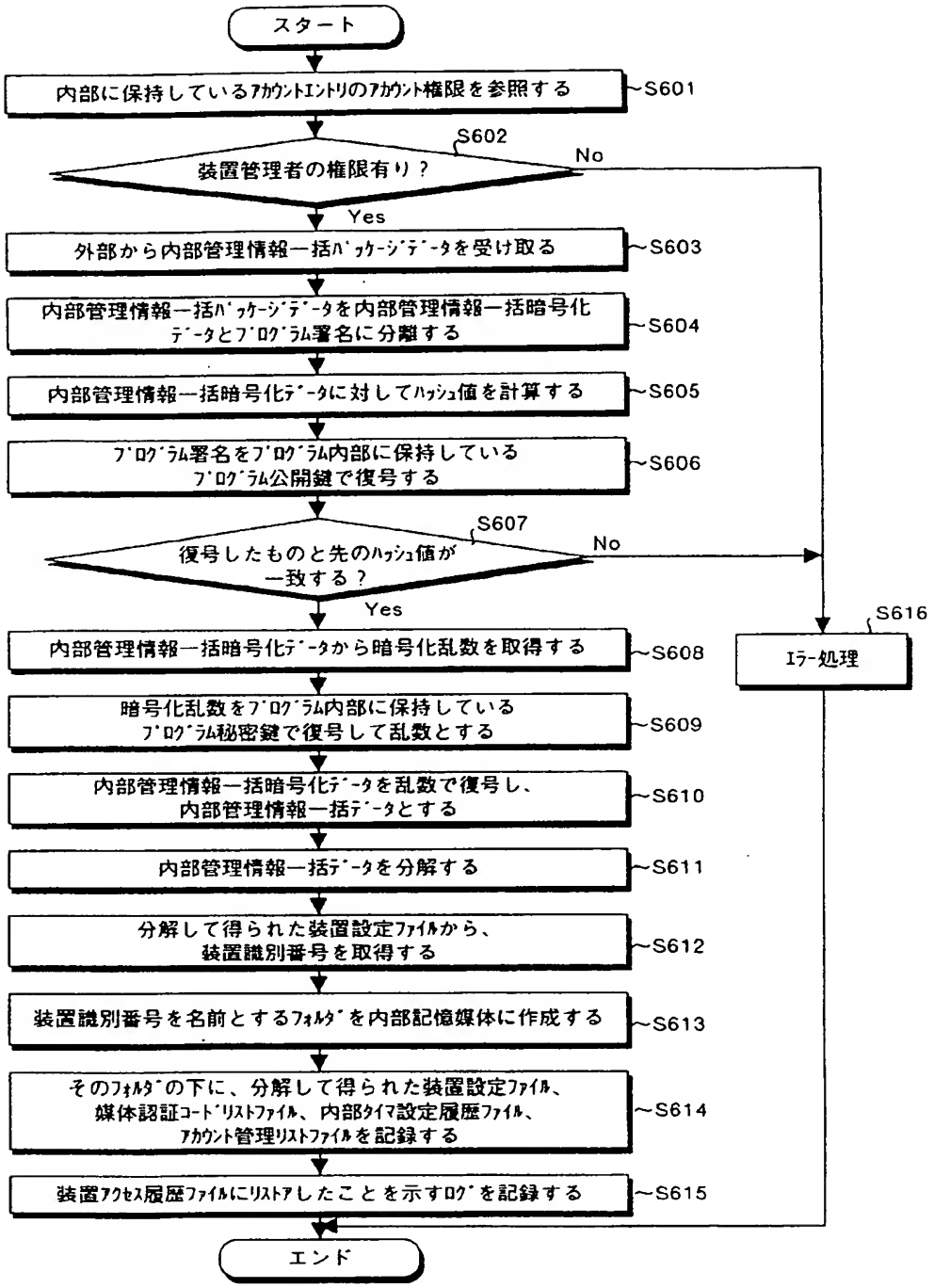
【図４】


スタート
内部に保持しているｱｶｳﾝﾄｴﾝﾄﾘの
ｱｶｳﾝﾄ権限を参照する
S401
S402
装置管理者のｱｶｳﾝﾄ
権限有り？
No
Yes
内部記憶媒体から装置設定ﾌｧｲﾙ、媒体認
証ｺｰﾄﾞﾘｽﾄﾌｧｲﾙ、内部ﾀｲﾏ設定履歴ﾌｧｲﾙ、
ｱｶｳﾝﾄ管理ﾘｽﾄﾌｧｲﾙを読み出す
S403
読み出したﾌｧｲﾙを一括して
内部管理情報一括ﾃﾞｰﾀとする
S404
乱数を生成する
S405
乱数をﾌﾟﾛｸﾞﾗﾑ内部のﾌﾟﾛｸﾞﾗﾑ公開鍵に
より暗号化し、暗号化乱数とする
S406
乱数により内部管理情報一括ﾃﾞｰﾀを
暗号化し、暗号化乱数を付与して
内部管理情報一括暗号化ﾃﾞｰﾀとする
S407
内部管理情報一括暗号化ﾃﾞｰﾀに
対してﾊｯｼｭ値を計算する
S408
ﾊｯｼｭ値をﾌﾟﾛｸﾞﾗﾑ内部のﾌﾟﾛｸﾞﾗﾑ秘密鍵に
より暗号化し、ﾌﾟﾛｸﾞﾗﾑ署名とする
S409
内部管理情報一括暗号化ﾃﾞｰﾀに
ﾌﾟﾛｸﾞﾗﾑ署名を付与し、内部管理情報
一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀとする
S410
内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀを
外部ｼｽﾃﾑに送出する
S411
S412
ｴﾗｰ処理
エンド

【図５】


スタート
内部に保持しているｱｶｳﾝﾄｴﾝﾄﾘのｱｶｳﾝﾄ権限を参照する
S501
S502
装置管理者の権限有り？
No
Yes
S503
完全に新しい原本性保証電子保存装置である？
No
Yes
外部から内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀを受け取る
S504
内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀを内部管理情報一括暗号化ﾃﾞｰﾀとﾌﾟﾛｸﾞﾗﾑ署名に分離する
S505
内部管理情報一括暗号化ﾃﾞｰﾀに対してﾊｯｼｭ値を計算する
S506
ﾌﾟﾛｸﾞﾗﾑ署名をﾌﾟﾛｸﾞﾗﾑ内部に保持しているﾌﾟﾛｸﾞﾗﾑ公開鍵で復号する
S507
S508
復号したものと先のﾊｯｼｭ値が一致する？
No
Yes
内部管理情報一括暗号化ﾃﾞｰﾀから暗号化乱数を取得する
S509
暗号化乱数をﾌﾟﾛｸﾞﾗﾑ内部に保持しているﾌﾟﾛｸﾞﾗﾑ秘密鍵で復号して乱数とする
S510
内部管理情報一括暗号化ﾃﾞｰﾀを乱数で復号し、内部管理情報一括ﾃﾞｰﾀとする
S511
内部管理情報一括暗号化ﾃﾞｰﾀを分解し、装置設定ﾌｧｲﾙ、媒体認証ｺｰﾄﾞﾘｽﾄﾌｧｲﾙ、内部ﾀｲﾏ設定履歴ﾌｧｲﾙ、ｱｶｳﾝﾄ管理ﾘｽﾄﾌｧｲﾙとして内部記憶媒体に記録する
S512
S517
ｴﾗｰ処理
外部から受け取った現在時刻で内部ﾀｲﾏを設定する
S513
設定前の日時情報を不明とし、設定後の日時情報を先に受け取った現在時刻にしたﾀｲﾏ設定ｴﾝﾄﾘを作成する
S514
内部ﾀｲﾏ設定履歴ﾌｧｲﾙに新しいﾀｲﾏ設定ｴﾝﾄﾘを追加する
S515
装置ｱｸｾｽ履歴ﾌｧｲﾙにﾘｽﾄｱしたことを示すﾛｸﾞを記録する
S516
エンド

【図６】


スタート
内部に保持しているｱｶｳﾝﾄｴﾝﾄﾘのｱｶｳﾝﾄ権限を参照する
S601
S602
装置管理者の権限有り？
No
Yes
外部から内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀを受け取る
S603
内部管理情報一括ﾊﾟｯｹｰｼﾞﾃﾞｰﾀを内部管理情報一括暗号化ﾃﾞｰﾀとﾌﾟﾛｸﾞﾗﾑ署名に分離する
S604
内部管理情報一括暗号化ﾃﾞｰﾀに対してﾊｯｼｭ値を計算する
S605
ﾌﾟﾛｸﾞﾗﾑ署名をﾌﾟﾛｸﾞﾗﾑ内部に保持している
ﾌﾟﾛｸﾞﾗﾑ公開鍵で復号する
S606
S607
復号したものと先のﾊｯｼｭ値が一致する？
No
Yes
S616
ｴﾗｰ処理
内部管理情報一括暗号化ﾃﾞｰﾀから暗号化乱数を取得する
S608
暗号化乱数をﾌﾟﾛｸﾞﾗﾑ内部に保持している
ﾌﾟﾛｸﾞﾗﾑ秘密鍵で復号して乱数とする
S609
内部管理情報一括暗号化ﾃﾞｰﾀを乱数で復号し、
内部管理情報一括ﾃﾞｰﾀとする
S610
内部管理情報一括ﾃﾞｰﾀを分解する
S611
分解して得られた装置設定ﾌｧｲﾙから、
装置識別番号を取得する
S612
装置識別番号を名前とするﾌｫﾙﾀﾞを内部記憶媒体に作成する
S613
そのﾌｫﾙﾀﾞの下に、分解して得られた装置設定ﾌｧｲﾙ、
媒体認証ｺｰﾄﾞﾘｽﾄﾌｧｲﾙ、内部ﾀｲﾏ設定履歴ﾌｧｲﾙ、
ｱｶｳﾝﾄ管理ﾘｽﾄﾌｧｲﾙを記録する
S614
装置ｱｸｾｽ履歴ﾌｧｲﾙにﾘｽﾄｱしたことを示すﾛｸﾞを記録する
S615
エンド